| Notice of Allowability | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/886,975 | BOOM, DOUGLAS D. | |
| | Examiner | Art Unit | |
| | Thomas M. Ho | 2132 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--***

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *8/28/06*.

2. ☒ The allowed claim(s) is/are *1-16,18,20,22-24,26,28,30 and 31*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   **Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

1. **Claims 1-16, 18, 20, 22-24, 26, 28, 30-31, 46-51 are pending.**

2. **The amendment of 8/28/06 has been received and entered.**

***Reasons For Allowance***

3. Claims 1-13, 14-16, 18, 20, 22-24, 26, 28, 30-31, 46-51 are held to be allowable.

Claim 1 recites:

*A computer having application software in communication with a network protocol, the computer comprising a network interface and a zombie detection driver coupled between, and in communication with, the network protocol and the network interface, the zombie detection driver comprising:*

- *A transmit module to receive outgoing packets from a software application and to discard the outgoing packets that are determined to be from a zombie application prior to being transmitted over a network.*

It is the Examiner's understanding that Applicant is claiming a computer having application software and a monitor such that outgoing data packets, transmitted from the purported "zombie application" are detected by the transmit module on the same computer prior to entering the network.

To this effect, the Applicant has argued that Schuba does not disclose this. Applicant asserts that Scuba monitors the TCP packets already along the network. Additionally the Applicant states that, Schuba, contrary to Applicant's invention, discloses a monitor and destination host as separate entities.

Applicant has argued: (page 21 last paragraph – page 22 first paragraph):

*...To the contrary, Schuba teaches detection and examination of TCP packets sent to a destination host by a monitor, wherein the monitor and the destination host are separate entities and the monitor monitors the TCP packets along the network.*

As stated above, the Applicant has claimed a transmit module which receives or "catches" outgoing data packets from an Application program or software application, and catches these packets prior to their transmission over the regular network.

Support for this interpretation is further evidenced by the Applicant's abstract within the specification

*Abstract:*

*More particularly, the present invention monitors packets being transmitted by a computer over a network and is able to identify when these packets are part of a distributed denial of service (DDOS) attack and is able to stop the transmission of these packets before they enter the network.*

In light of the Applicant's amendments, it is the Examiner's position that Schuba fails to disclose such a transmission module to further comprise the zombie detection driver, which is stated as "coupled between" the network protocol and the network interface.

No additional art has been found which discloses this limitation, nor has any motivation been found to render the invention to the limitations as claimed by the Applicant in claim 1. Accordingly, claim 1 is held to be allowable.

Claims 2-9, 30, 31 are dependent claims which depend on claim 1 or a dependent of claim 1 thereof. Accordingly, these claims are held to be allowable.

Claims 10-13 recite the limitation

*"the zombie rating being based on whether the software application is an application or a process and whether the software application is user initiated or initiated at system startup."*

While Schuba does disclose a "zombie rating" for a particular program which manages hardware which transmits outgoing data packets, the rating of Schuba is dependent upon the behavior of particular hosts (Column 11, lines 5-15), and not whether the software application is user initiated or initiated at system startup.

No additional art has been found which discloses this limitation, nor has any motivation been found to render the invention to the limitations as claimed by the Applicant in claims 10-13.

Accordingly, claims 10-13, 50 and their dependent claims 46- 49, 51 are allowable.

In reference to claim 14:

Schuba et al. discloses a method of detecting and restricting denial of service attacks comprising:

- Monitoring incoming and outgoing packets to and from a software application, where the monitored packets are the monitored data streams. (Column 9, lines 15-32) (Column 5, lines 58 – Column 6, line 8)
- Placing the software application on a zombie list or a watch list when a pattern of the incoming or outgoing packets to or the software application matches that of the characteristics of a zombie application, where the zombie list is the list (Column 6, lines 30-37) from where the hosts have a rank. (Column 11, lines 8-15)
- Determining whether the software application is a known good application, wherein if the software application is not a known good application, then applying a zombie rating to the software application and if the software application is a known good application, then removing the software application from the watch list and/or zombie list, where the software application is determined to be good or bad/evil ("zombie"), and where this rating is placed as a list in a database, and where if the software application is reclassified

as a good application, the good application is removed from its status as a bad address. (Column 11, lines 50-67) & (Column 12, lines 15-32) & (Column 8, lines 18-33)

- Blocking reception and transmission of packets to and from the software application when the software application has been placed on the watch list or the zombie list in a previous cycle and the software application further exhibits the characteristics of a zombie application. (Column 11, line 65 – Column 12, line 32) & (Column 8, lines 18-33)

Schuba et al. fails to explicitly disclose a software application. Rather, Schuba monitors and classifies packets coming from specific network addresses or client systems.

However, one of ordinary skill in the art would recognize that receiving packets from a network address necessitates the packets were generated at a client computer, where the packets sent were transmitted from hardware that was operated by a control program.

For Example, if disclosure was made in which a web server receives a request for a website, one of ordinary skill in the art would recognize that the request was generated using application software such as a web browser (Internet Explorer, Netscape, Opera, Firefox).

As an additional example, Scuba et al. discloses the hardware apparatus which is operated by a set programming. (Column 7, lines 15-50)

All application programs and software inherently control and direct the use of hardware, as per the instructions dictated by its internal source code within. The advantage of using programs to control hardware is that it allows for more convenient and complex control.

It would have been obvious to one of ordinary skill in the art at the time of invention to monitor packets deriving from a software application, where the software application was operable to control a specific set of hardware to initiate the transmissions, in order to better operate and control the hardware.

Schuba et al. however additionally fails to disclose:
Determining whether the software application is a known good application wherein if the software application is not a known good application, then applying a zombie rating to the software application, wherein the zombie rating is based on the factors of whether the software application is an application or a process and whether the software application is user initiated or initiated at system startup.

A search of the prior art has not found an embodiment where a zombie rating is based on the factors of whether the software application is an application or a process and whether the software application is user initiated or initiated at system startup. Accordingly claim 14 is allowable.

The rejection under 35 USC 101 has been withdrawn with respect to claims 22-24, 26, 28 in view of the amendments made in the communication of 8/28/06.

Claim 22 is allowable for the same reasons as claim 14.

Claims 15, 16, 18, 20 are allowable because they depend on claim 14.

Claims 23, 24, 26, 28 are allowable because they depend on claim 22.

***Conclusion***

4. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on **(571)272-3799.**

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

| | | |
|---|---|---|
| General Information/Receptionist | Telephone: 571-272-2100 | Fax: 571-273-8300 |
| Customer Service Representative | Telephone: 571-272-2100 | Fax: 571-273-8300 |

TMH

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100